

FIG. 1

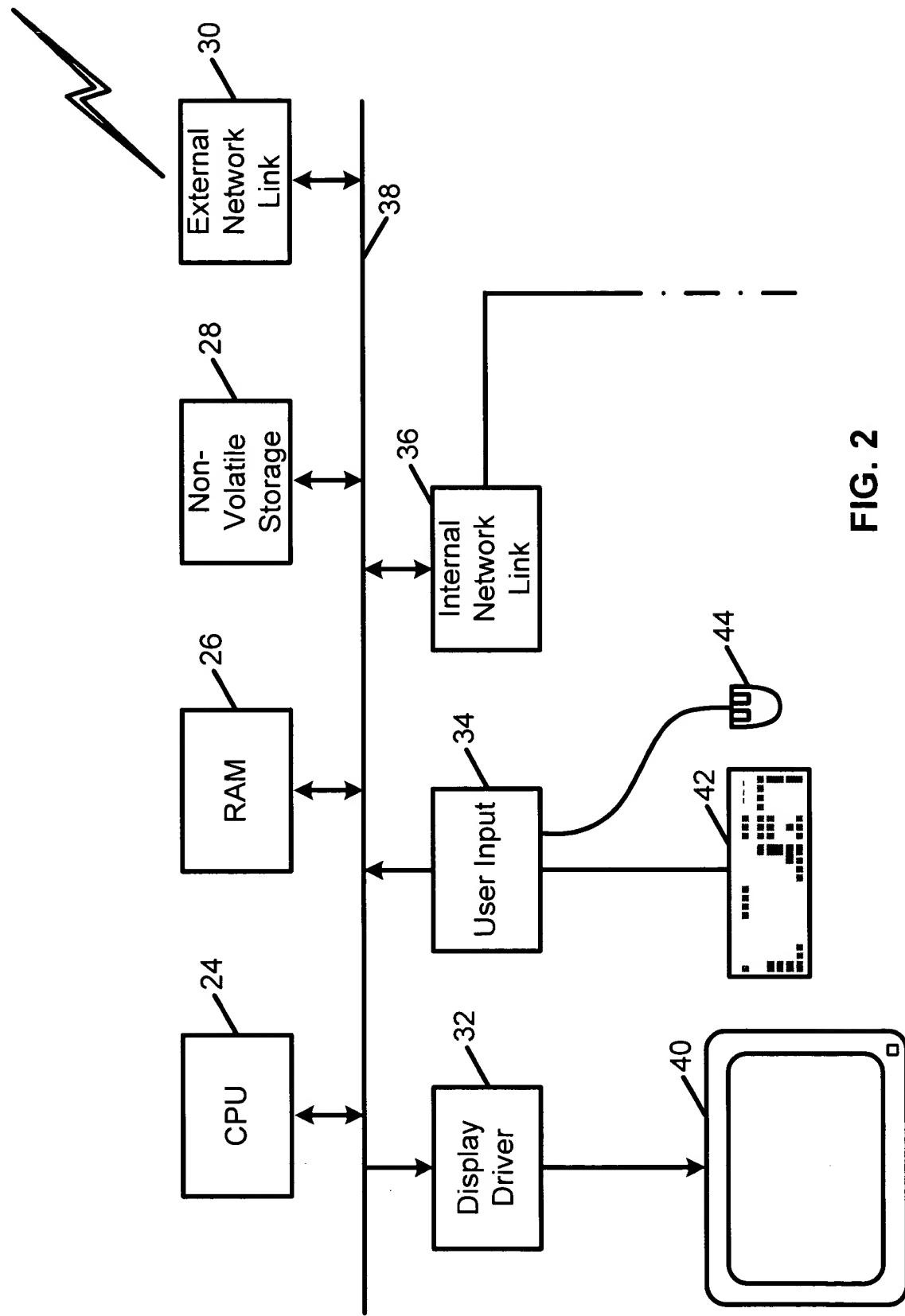


FIG. 2

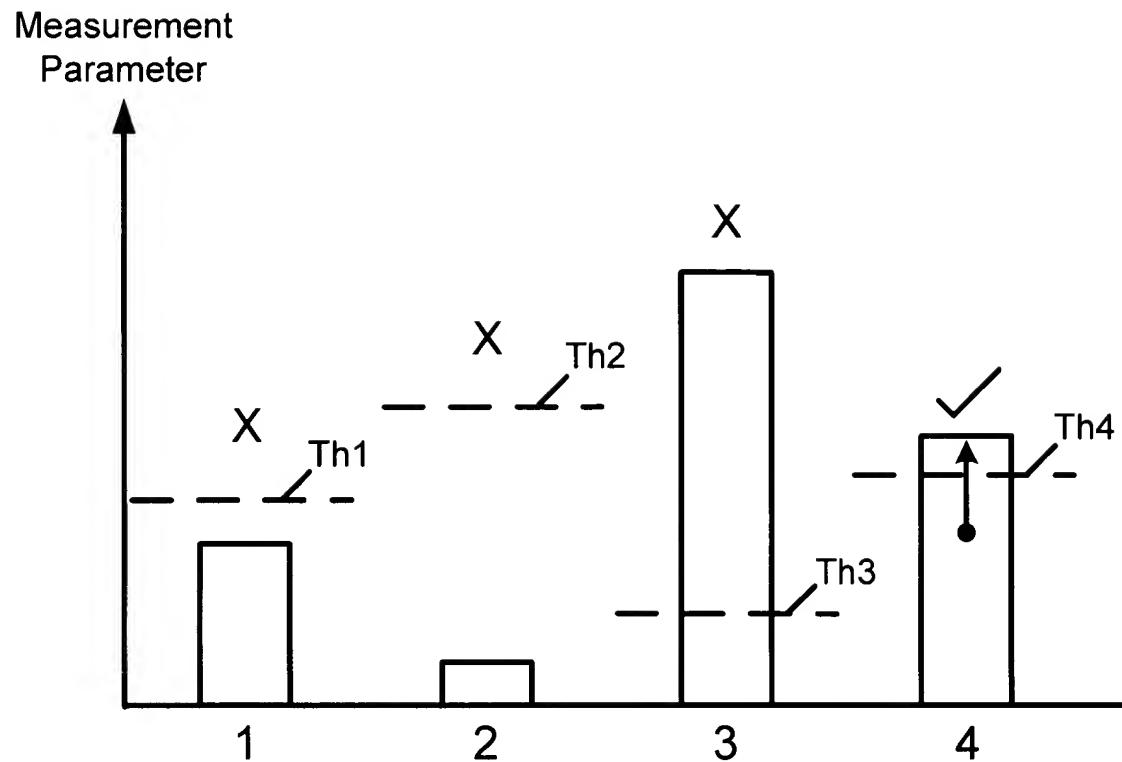


FIG. 3

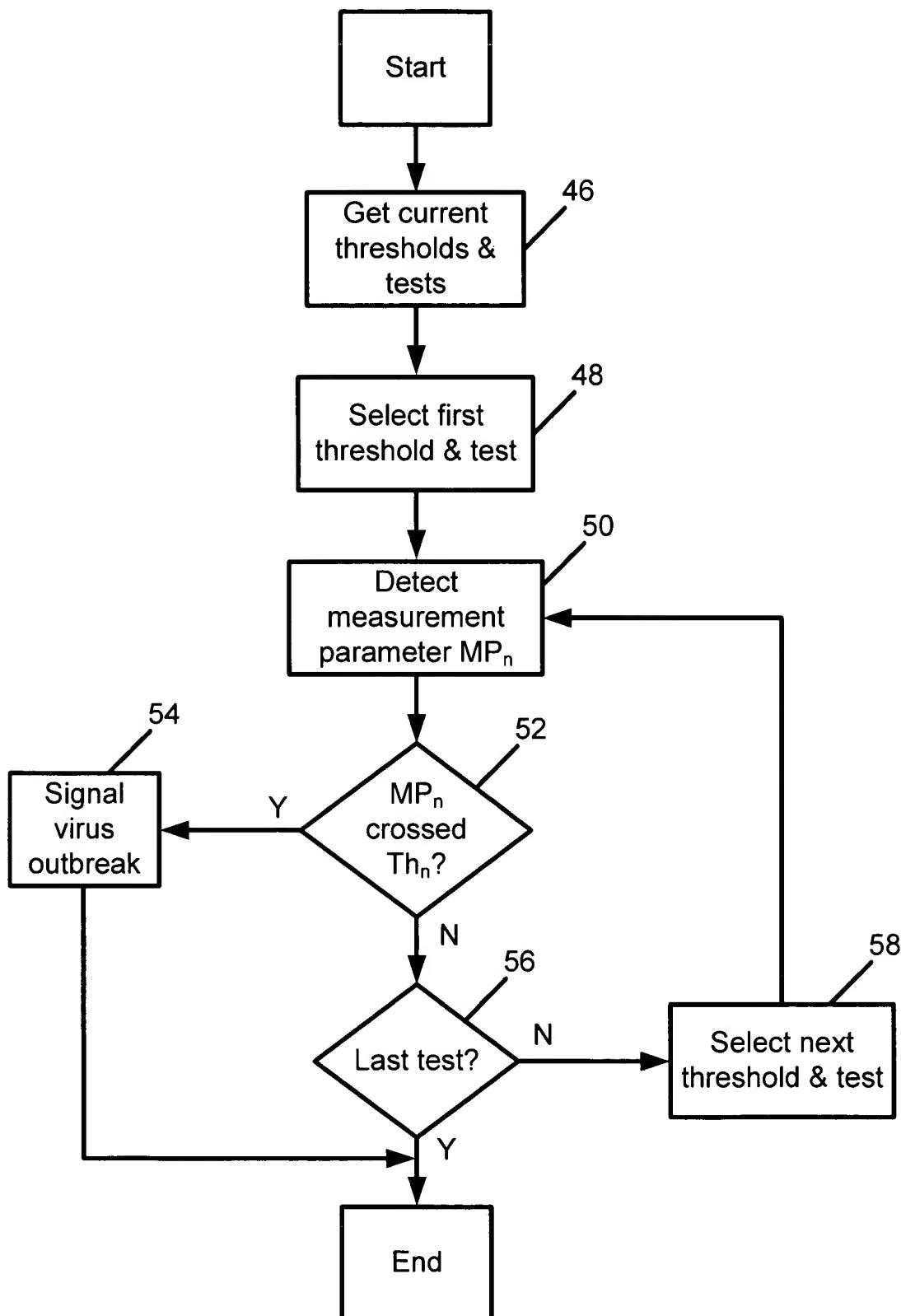
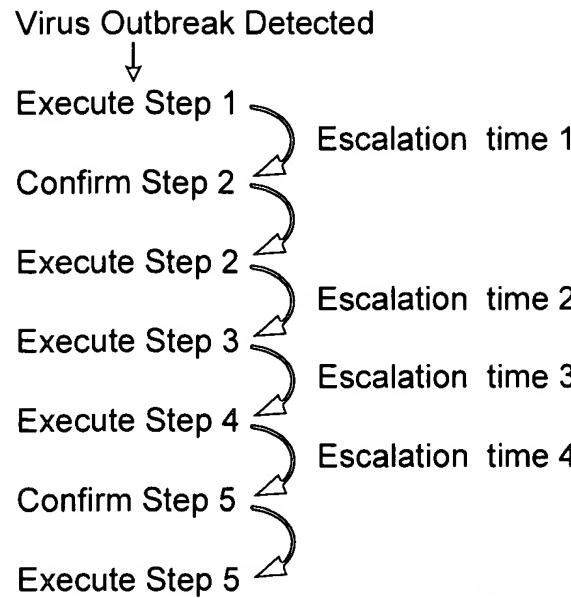


FIG. 4



Legend:

Predefined Actions To Be Followed Upon Detection of Outbreak

Such actions may optionally include:

1. Reducing virus detection notification;
2. Switching from virus quarantining to virus deletion when a computer virus is detected;
3. Increasing scan options that control how thoroughly the computer system is scanned to detect a computer virus;
4. Sending a copy of the detected computer virus to a remote site for analysis;
5. Downloading a latest virus definition file from a remote site;
6. Performing a complete virus scan of all computer files stored in at least a portion of the computer apparatus;
7. Blocking e-mail attachments to block identical attachments appearing in excess of a threshold level;
8. Rendering non-accessible e-mail distribution lists and e-mail address books of e-mail clients coupled to the computer apparatus;
9. Restarting in administrator mode an e-mail post office coupled to the computer apparatus; and
10. Closing down an e-mail post office coupled to the computer apparatus.

FIG. 5

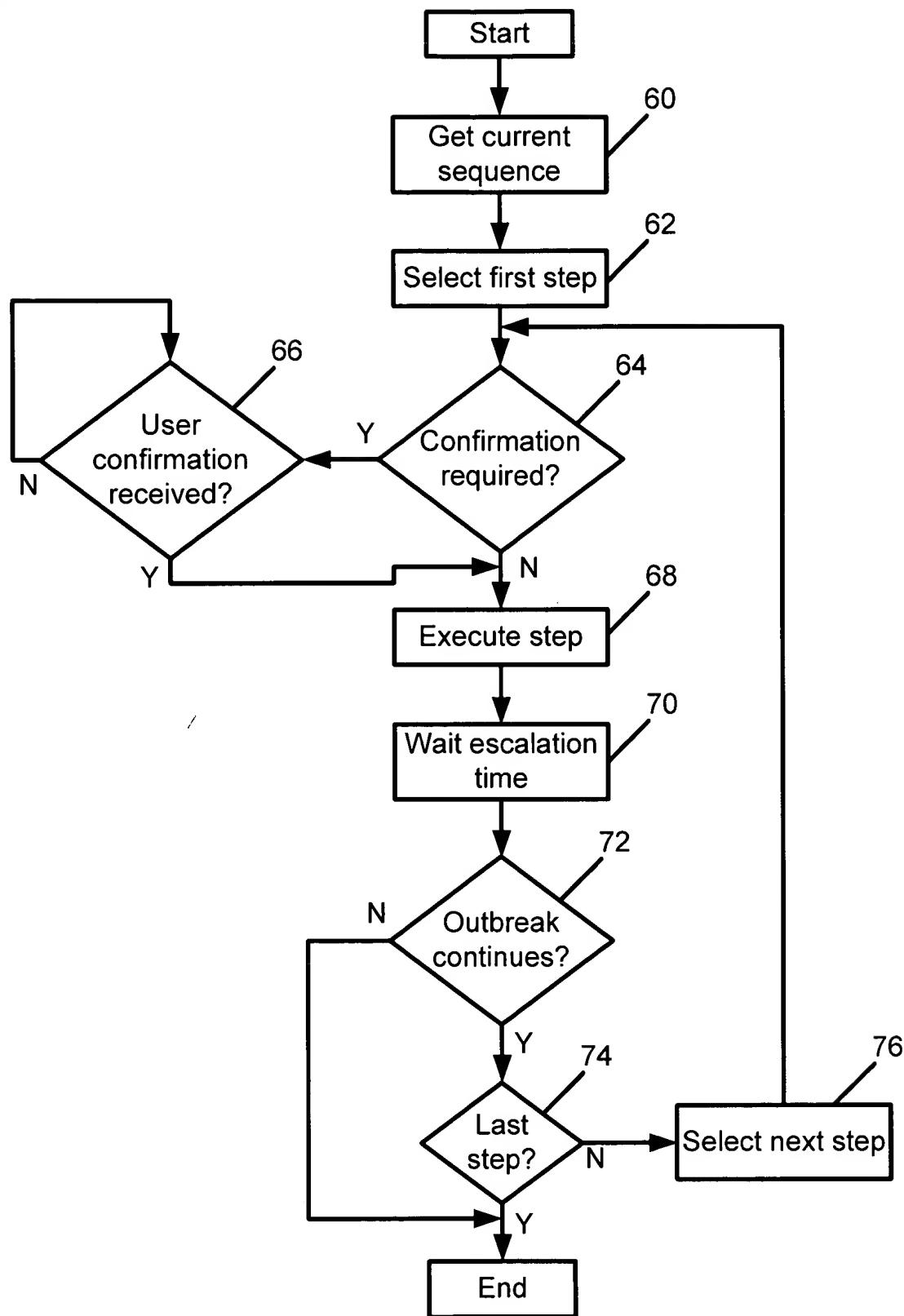


FIG. 6



Network Associates Emergency Response

Apply rules in the following order:

Outbreak response stage 1
Outbreak response stage 2

New
Copy
Modify
Rename
Delete

Move Up Move Down

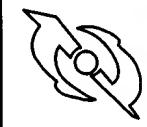
Event description (click on an underlined value to edit it)

OK Cancel

FIG. 7

Emergency Response Event

Which type of event do you wish to create?


Number of Identical Attachment types in a Time Period
Number of Identical Attachments in a Time Period
Number of Identical Viruses in a Time Period
Number of Viruses in a Time Period

Event description (click on an underlined value to edit it)

Number of virus(es) in 1 hours 20 minutes

< Back Next > Cancel Help

FIG. 8



Number

Please enter the new numeric value :

5

OK Cancel

Time

Please enter the new time value :

Hour(s): Minute(s)

1 20

OK Cancel

FIG. 9

Threshold

Threshold Scale Values

Threshold

Threshold

Mon Tue Wed Thu Fri Sat Sun

FIG. 10



Emergency Response Event

Which type of reaction do you wish for this event?

Manual
 Automatic

Notify by email
 Notify by network broadcast
 Notify by pager

Reaction description (click on an underlined value to edit it)

React manually to an emergency response but notify me via email address email address

< Back Next > Cancel Help

FIG. 11

Number

Please enter the new numeric value :

3028423555111

OK Cancel

FIG. 12

Email Address

Please enter the new email address :

a@a.com

OK Cancel

FIG. 13



Machine name

Please enter the new machine name :

AYL-NOBODY

OK Cancel

FIG. 14

Out of office hours

Please enter the out of office hours :

Day	Am	12	1	2	3	4	5	6	7	8	9	10	11	12	Noon	1	2	3	4	5	6	7	8	9	10	11	Pm
Monday																											
Tuesday																											
Wednesday																											
Thursday																											
Friday																											
Saturday																											
Sunday																											

Sunday – 7 am

OK Cancel

FIG. 15



Emergency Response Event

Specify the actions and step to carry out:

Step	Action	Escalation Time
0	Update DAT files (GroupShield Exc...)	0 hr(s) 1 min(s)
1	Reduce notifications (GroupShield ...)	0 hr(s) 10 min(s)

Create an emergency response report

FIG. 16

Available Actions

Component	Action
GroupShield Exchange	Delete on Infection
GroupShield Exchange	Reduce notifications
GroupShield Exchange	Hide Mailboxes
GroupShield Exchange	Hide distribution lists
GroupShield Exchange	Perform On-Demand Scan
GroupShield Exchange	Update DAT files
GroupShield Exchange	Down the Exchange Server
GroupShield Exchange	Increase Scanning Options

Escalation Time —

Escalate after : hr(s) min(s)

FIG. 17



Emergency Response Event

Specify the name for this event :

Event1

Event Summary :

Event Name : 'Number of Identical Attachment types in a Time
Event Desc : 500 identical attachment types in 1 hours 20 minu
Reaction to an Emergency is Automatic
Email Notification is Enabled. Email will be sent to 'a@a.com'

Automatic Actions

Step, Action and escalation times

0 Update DAT files (0 hr(s) 1 min(s))

< Back Finish Cancel Help

FIG. 18

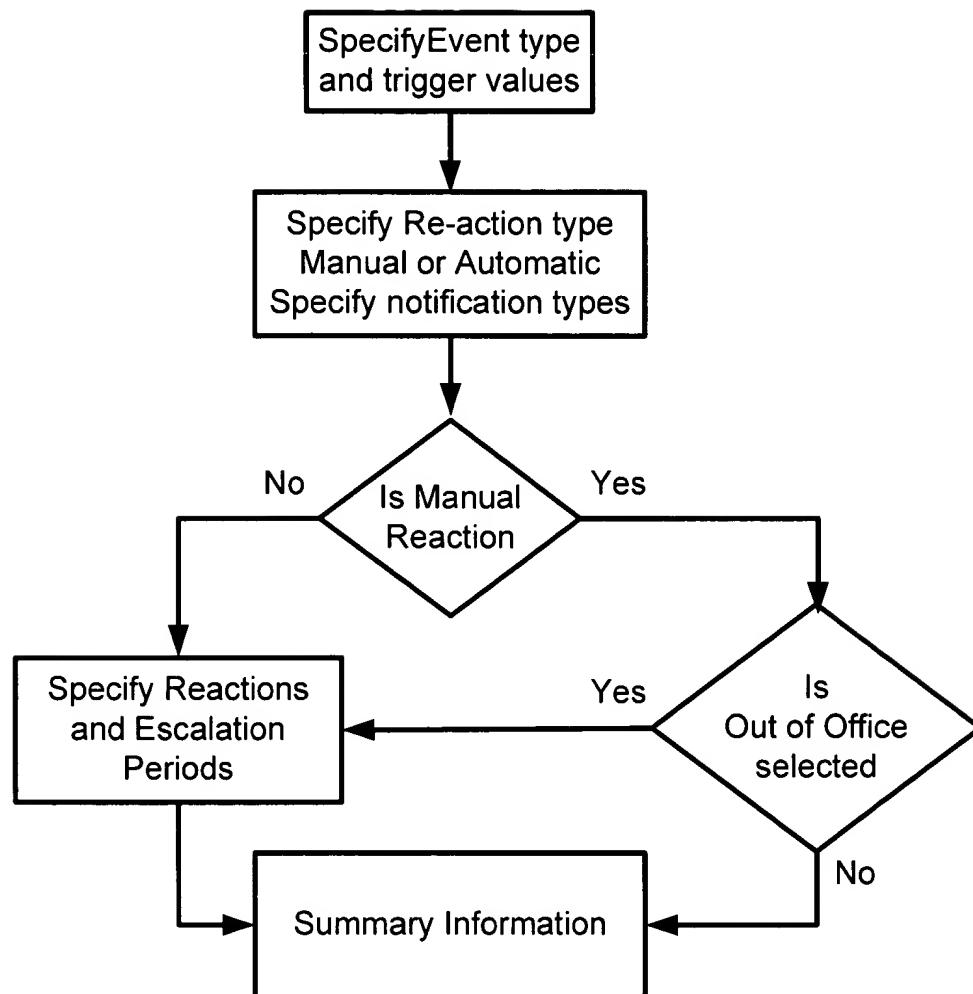


FIG. 19



FIG. 20

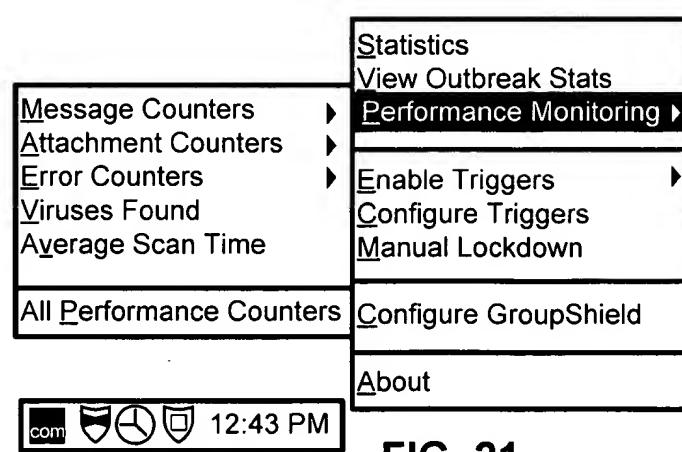


FIG. 21



Outbreak Statistics					
Attachment Name	Attachment Size	Occurrences	Virus Type	Virus Name	Time
ABC.doc	1034	2	MACRO	WMCAPI	10:45:45
XYZ.exe	4096	10	FILE	Bomber	21:19:32

FIG. 22



Lockdown	<input checked="" type="checkbox"/>
Network Associates has determined a virus Outbreak based on the currently defined triggers. What action would you like to take?	<input type="button" value="OK"/> <input type="button" value="Cancel"/>
<ul style="list-style-type: none"><input checked="" type="radio"/> None<input type="radio"/> Turn down notification options to reduce load on the server<input type="radio"/> Increase security on scanning options<input type="radio"/> Perform a DAT update to retrieve latest detection and clean<input type="radio"/> Perform an on-demand scan<input type="radio"/> Block all attachments by trigger<input type="radio"/> Perform an on-demand scan<input type="radio"/> Allow only one Admin to logon to Exchange<input type="radio"/> Down Exchange	<p>Recommendation by GroupShield : _____</p> <p>Perform an dat update from Network Associates FTP site</p>

FIG. 23